Deloitte.

# Cryptographic Resilience

**A Cyber Security Framework (CSF) 2.0 Community Profile**

April 2025

# Table of contents

# Introduction

## Purpose and Scope

This publication seeks to assist organizations to understand and advance cryptographic resilience as part of their overall cybersecurity risk management activities, as defined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.[1] For purposes of this document, cryptographic resilience primarily refers to achievement of organizational performance outcomes that enable a prioritized migration to quantum-resistant cryptography (QRC) and transition to cryptographic agility.[2] This document was produced as a starting point for strategic communications to executive leadership on this topic, leveraging a mechanism that has demonstrated commercial effectiveness. We hope that an outcome of this will be that quantum cyber risk is understood throughout organizational levels and more closely aligned to general cyber hygiene activities – allowing for commensurate budget decisions to be made.

Achieving these performance outcomes can enable organizations to advance their quantum cyber readiness and prepare for the potentially destructive threats that future cryptanalytically-relevant quantum computers (CRQCs) pose to public-key cryptography. It can also help organizations address the challenges and opportunities to mission and business processes presented by the large-scale information technology (IT) transformations that may be necessitated by the implementation of QRC.

These connections to executive awareness and to business processes are the most important purpose of this document. Too often, discussions of quantum cyber readiness descend quickly into discussions of specific algorithms and/or when exactly a cryptanalytically-relevant quantum computer will exist. As illustrated in Figure 1 below, it is important to connect the use of cryptography across implementation parameters, from cryptographic algorithms themselves up to the business outcomes being achieved. This allows the correct focus and prioritization to be achieved in line with business objectives.

Given the embedded nature of vulnerable cryptography throughout an enterprise, the transition to QRC and cryptographic agility will be costly, time-intensive, and pose substantial interoperability issues that have high potential to disrupt operations. However, by adopting the CSF 2.0 Functions, Categories, and Subcategories (described further below) as a model for cryptographic resilience, organizations can take a performance outcomes-based approach to quantum cyber readiness that fosters collaboration and innovation and mitigates the risks of IT implementation. Such a model is all the more imperative due to the volume of individuals, teams, and third parties that hold a wide variety of roles and responsibilities across all of the Functions that support an organization's cryptographic resilience. Finally, such a model can offer critical guidance to organizations should they determine that compliance-based processes, frameworks, and controls are currently inadequate or unsuitable for the quantum era, whether due to the uncertainty surrounding threat timelines, their likely rapid evolution, and/or the nascency of technology solutions available to address them.

Using the CSF, each organization can tailor their approach to cryptographic resilience in a manner that meets their mission and business needs, including through the development of organizational and target profiles. This model can be built on further to accommodate the unique demands of an organization's interconnected digital ecosystem, through the development of CSF Industry Profiles.

## Document Structure

This document consists of Section 1: CSF Tiers and Section 2: CSF Community Profile, each designed with an understanding that different organizations are at different phases of their quantum cyber readiness journeys.

Section 1 introduces a tiered approach to inform how organizations can achieve quantum cyber readiness. It tailors the NIST CSF 2.0 Tiers to Cryptographic Resilience, which can be applied to characterize the rigor of an organization's cybersecurity risk governance and management practices. These tiers can also provide context for how an organization views and assesses cybersecurity risks and the processes in place to manage those risks.

Section 2 contains a baseline of priority CSF performance outcomes that focus on the shared interests and goals of organizations that are seeking to mitigate the threat to cryptography posed by the emergence of a CRQC. Given the breadth of this

community, this baseline contains an initial set of performance outcomes that are likely most impactful and timely for a broad set of organizations today, considering today's threat and technology landscape (whether large government agencies, or a small to mid-sized business). This baseline will be updated as both the threat and solution landscape evolve.

Organizations should use this document with reference to the NIST CSF 2.0, NIST Federal Information Processing Standards (FIPS), and guidance concerning cryptography and cryptographic agility and management. [3]

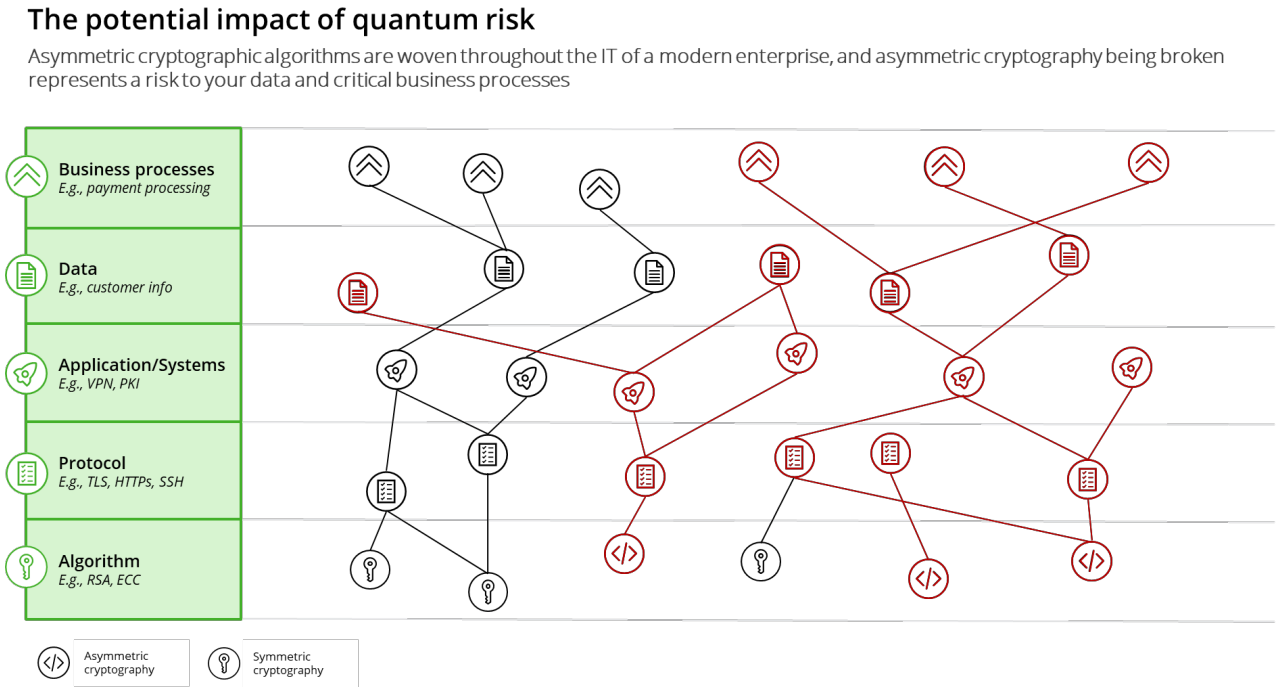


Figure 1. How post-quantum cryptographic risk maps to organizational data and business processes.

 

# CSF Tiers

## A differentiated approach to cryptographic resilience

Based on the NIST CSF 2.0, and in alignment with other frameworks that specifically address cryptographic agility and resilience (such as the CISA Zero Trust Maturity Model 2.0),[4] the tiers described in Table 1 below can be used to demonstrate an organization's practices for managing quantum cyber risk. The Tiers reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving.

Organizations may use the tiers to benchmark their approach to managing cryptographic risk and to plan their progression to greater cryptographic resilience. When applied in conjunction with the performance outcomes in the Profile below, organizations can adapt their cyber risk management methodology to prioritize cryptographic resilience, regardless of the current state of their governance and risk management capabilities.

*Table 1: Cryptographic Resilience Tiers*

| Tier Description | Expected Risk Governance and Risk Management Characteristics |
|---|---|
| **Tier 0: Basic.** Limited visibility into cryptographic risk across the enterprise. | • The organization has identified some CRQC-vulnerable systems and services, devices, networks, applications, and data that use asymmetric cryptography, including across public key infrastructure (PKI), and has defined some policies and procedures related to cryptographic risk, including QRC.<br>• Risk is not prioritized, and only limited capabilities for cryptography management and maintenance are implemented. |
| **Tier 1: Partial.** General awareness of quantum threats. Governance of quantum cyber readiness is minimal and ad hoc. | • The organization has knowledge of and understands the cryptographic algorithms in use on their systems and services, devices, networks, applications, and data, and has strategies and roadmaps in place to guide cryptographic migration.<br>• Limited capabilities for cryptographic resilience are implemented, however, efforts are reactive and lack coordination. This includes only limited inventorying and monitoring of CRQC-vulnerable cryptography.<br>• Prioritization of risk is ad hoc and not formally based on objectives or threat environment. |
| **Tier 2: Risk Informed.** Enterprise-level awareness of quantum threats. Formalized processes for cryptographic resilience. | • The organization is manually inventorying and reporting on its identified CRQC-vulnerable cryptography, including those related to its supply chains.<br>• It has established a program management office (PMO), cryptographic center of excellence (CoE) or equivalent governance structure for quantum-resistant cryptography (QRC) migration and for incorporating cryptographic-agility into environmental changes.<br>• Capabilities for quantum cyber readiness are established across the enterprise and informed by risk assessments, although there is limited visibility to correlate risk across interconnected systems and business processes. |
| **Tier 3: Repeatable.** Consistently implemented processes for cryptographic resilience and monitoring of quantum cyber risks. | • The organization has a centralized mechanism for identifying, monitoring, and reporting on its CRQC-vulnerable cryptography, along with the ability to measure the effectiveness of its quantum cyber readiness (e.g., through benchmarking and ongoing assessment).<br>• QRC and solutions for cryptographic agility are tested and partially implemented across the enterprise, and feedback on effectiveness is monitored on an ongoing basis. |
| **Tier 4: Adaptive.** Proactive and agile solutions for cryptographic resilience and quantum cyber readiness. | • The organization leverages automation to discover and inventory in-use cryptography, integrating these processes into ongoing monitoring and mitigation efforts.<br>• Automation is used to facilitate QRC migration, including the implementation of orchestration capabilities.<br>• QRC and solutions for cryptographic agility are incorporated throughout the enterprise based on risk, including across the supply chain. |

 

# CSF 2.0 Community Profile

## Background

A CSF Community Profile is a baseline of NIST CSF performance outcomes that address shared interests and goals for reducing cybersecurity risk among a number of organizations. The NIST CSF 2.0 Functions organize cybersecurity performance outcomes at their highest level as follows:

- **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization's current cybersecurity risks are understood.
- **Protect (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

All six Functions have vital roles in cryptographic resilience and quantum cyber readiness, specifically:

- **Govern** provides a holistic structure to facilitate the transition to QRC and implement long-term strategies for cryptographic agility and resilience.
- **Identify** helps organizations to assess cryptographic risk throughout the enterprise to inform a prioritized migration to QRC and implementation of cryptographically agile solutions.
- **Protect** helps organizations to effectively implement QRC and other measures to safeguard data and systems from quantum threats.
- **Detect, Respond, and Recover** provide a framework for incorporating quantum cyber risk into an organization's broader cybersecurity monitoring and incident response programs.

## Overview

This section presents a CSF 2.0 Community Profile that consists of Cryptographic Resilience Recommendations for Quantum Cyber Readiness. It uses the CSF as the basis for highlighting and prioritizing cybersecurity performance outcomes that are important for achieving cryptographic resilience. It makes recommendations and provides considerations for implementation.

The Community Profile is split into four subsections. The first three sections separately cover the CSF categories of Govern, Identify, and Protect, and include tables with applicable CSF Categories and Subcategories, including performance outcomes and detailed recommendations and considerations. For each of these first three Functions, the Profile includes a targeted, initial set of Categories and Subcategories that are likely most impactful and timely for a broad set of organizations to advance their cryptographic resilience. All the included Categories and Subcategories described in the tables below should be considered by most organizations as High priority, and core to cryptographic resilience.

The last section covers the CSF Functions of Detect, Respond, and Recover, and provides a high-level set of recommendations and considerations for organizations. Although the Categories and Subcategories under the last three Functions are expected to become more urgent in the future, particularly when organizations need to respond to and recover from widespread CRQC-based attacks, current prioritization of proactive measures is crucial for organizations to enhance cryptographic resilience and prevent cryptographic incidents from the start. Apart from one Category, Continuous Monitoring (DE.CM), they can therefore be considered by most organizations as Moderate to Low priority and not core to cryptographic resilience today.

This Community Profile is intended for use by organizations regardless of sector or size. Organizations should use an approach to cryptographic resilience that aligns to their business and mission needs and may determine that not every recommendation and consideration detailed below applies to their business and IT environment. However, every organization should take cryptographic resilience into consideration throughout their cybersecurity risk management activities, particularly as they work to achieve quantum cyber readiness. By aligning the recommendations in this document to the CSF 2.0, organizations can leverage the wealth of resources available for CSF 2.0 and integrate with CSF-related activities in which they may already be engaged.

 

## Govern

The Govern (GV) Function emphasizes the critical importance of establishing, communicating, and monitoring an organization's cybersecurity risk management strategy, expectations, and policies. It includes the following Categories, which provide key performance outcomes as part of a broad cyber risk management framework:

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.
- **Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.
- **Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.
- **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced.
- **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.
- **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

As detailed in the table below, addressing each of the Govern Categories and associated Subcategories is key for effective cryptographic resilience as organizations advance their quantum cyber readiness. Specifically, as quantum computing advances, the potential threats to current cryptographic systems necessitate a proactive and robust governance framework. This includes understanding the organizational context, defining risk management strategies, and maintaining compliance with legal, regulatory, and contractual requirements. A deep understanding of the organizational mission, internal and external stakeholders, and technical dependencies on CRQC-vulnerable cryptography is critical to informing risk prioritization and QRC migration planning.

*Table 2: CSF 2.0 Community Profile – Govern*

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| GV.OC-01 | The organizational mission is understood and informs cybersecurity risk management | Mission context should be incorporated into cryptographic discovery and monitoring, as well as migration planning. Organizations should conduct a thorough assessment of how QRC and quantum cyber risk impacts the organizational mission and integrate findings into the cybersecurity risk management strategy. Mission priorities should inform the selection and implementation of QRC solutions – accounting for system interoperability and performance, in particular. |
| GV.OC-02 | Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered | Stakeholder dependencies should be incorporated into cryptographic discovery and monitoring, as well as migration planning. Organizations should conduct a thorough assessment of how QRC and quantum cyber risk impacts stakeholders and integrate findings into the cybersecurity risk management strategy. Stakeholder impacts should inform the selection and implementation of QRC solutions – accounting for system interoperability, performance, and trust, in particular. |
| GV.OC-03 | Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil | Organizations should review and update legal, regulatory, and contractual requirements to include QRC. Where organizations depend on third-parties for managing cryptographic risk, or carry cryptographic risks for extended time periods, proactive incorporation of QRC standards can provide significant risk reduction and cost savings in the long-term. |

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| | liberties obligations — are understood and managed | |
| GV.OC-04 | Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated | Critical objectives, capabilities, and services that stakeholders depend on, and that may be impacted by QRC migration and quantum cyber risk (including business processes, data, applications/systems, and underlying protocols and cryptographic algorithms), should be accounted for as part of cryptographic discovery and monitoring, as well as QRC migration planning. This should include dependencies with and across third-party stakeholders, such as information technology and public key infrastructure providers. Impacts should be incorporated into the organization's cybersecurity risk management strategy.<br><br>Organizations should consider impacts to system interoperability, performance, cost, and trust when selecting and implementing QRC and cryptographically agile solutions. For example, based on results of cryptographic discovery, an organization may determine that costs of proactive, multi-year implementations of QRC may be significantly less than a rapid, reactive migration and mitigation following emergence of a CRQC. In addition, organizations may find that the ongoing costs and risk from maintaining and operating systems with high cryptographic debt and rigidity may exceed the costs of transitioning to and operating cryptographically agile system architectures. Understanding and communicating the potentially significant value and cost savings associated with buying down cryptographic debt, regardless of the emergence of the CRQC, may be critical to achieving organizational objectives. |
| GV.OC-05 | Outcomes, capabilities, and services that the organization depends on are understood and communicated | Organizational outcomes, capabilities, and services that may be impacted by QRC migration and quantum cyber risk (including business processes, data, applications/systems, and underlying protocols and cryptographic algorithms), should be accounted for as part of cryptographic discovery and monitoring, as well as QRC migration planning. This should include dependencies with and across third-party stakeholders, such as information technology and public key infrastructure providers. Impacts should be incorporated into the organization's cybersecurity risk management strategy.<br><br>Organizations should consider impacts to system interoperability, performance, cost, and trust when selecting and implementing QRC and cryptographically agile solutions. For example, based on results of cryptographic discovery, an organization may determine that costs of proactive, multi-year implementations of QRC may be significantly less than a rapid, reactive migration and mitigation following emergence of a CRQC. In addition, organizations may find that the ongoing costs and risk from maintaining and operating systems with high cryptographic debt and rigidity may exceed the costs of transitioning to and operating cryptographically agile system architectures. Understanding and communicating the potentially significant value and cost savings associated with buying down cryptographic debt, regardless of the emergence of the CRQC, may be critical to achieving organizational objectives. |
| GV.RM-01 | Risk management objectives are established and agreed to by organizational stakeholders | Risk management objectives should incorporate, but not be limited to, QRC implementation. They should broadly address quantum cyber readiness, to include objectives for cryptographic agility, ongoing cryptographic discovery and management, as well as alignment to related risk management activities such as privacy, secure supply chain and Zero Trust. |
| GV.RM-02 | Risk appetite and risk tolerance statements are established, communicated, and maintained | Risk appetite and tolerance statements should address both implementation of QRC and depreciation of legacy cryptographic algorithms. They should address timelines for implementation and depreciation and should be updated to account for new QRC algorithms and capabilities.<br><br>There is not a one-size-fits-all approach to quantum cyber risk management. As such, risk appetite and tolerance statements should be tailored to an organization's mission and business needs and differentiated across assets, particularly depending on factors such as whether cryptography is |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| | | embedded in hardware or software, or whether assets are custom-built or commercial off-the-shelf products.<br><br>Risk appetite and tolerance statements should be communicated proactively to stakeholders involved in acquisitions and third-party risk management so that quantum cyber risk can be addressed early in IT acquisition lifecycles. |
| GV.RM-03 | Cybersecurity risk management activities and outcomes are included in enterprise risk management processes | A Quantum Cyber Readiness Strategy and Roadmap should be established that broadly addresses QRC across the enterprise, and accounts for people, processes, and technology. It should include activities for cryptographic agility, ongoing cryptographic discovery and management, as well as alignment to related risk management activities such as privacy, secure supply chain, and Zero Trust.<br><br>Cryptographic risk should be addressed and documented throughout organizational risk management (e.g., Governance, Risk, and Compliance (GRC)) processes. This can include tracking readiness for QRC implementation in organizational risk registers and risk remediation documentation (e.g., Plans of Action and Milestones (POA&M)). |
| GV.RM-04 | Strategic direction that describes appropriate risk response options is established and communicated | A Quantum Cyber Readiness Strategy and Roadmap should establish thresholds and approaches for risk determination, as well as acceptance and mitigation decisions.<br><br>Risk decisions should be made with concurrence from the senior-most official with responsibility over the ecosystem of business processes impacted by the applicable cryptographic assets. Risk decisions should address interoperability and availability risks associated with QRC migration and cryptographic compromise, not only risks associated with vulnerability of specific cryptographic assets.<br><br>Piloting QRC technologies and new cryptographically agile and hybrid solutions and architectures, as well as conducting workshops to explore approaches to cryptographic risk management, can inform risk decisions and increase confidence in implementation. |
| GV.RM-05 | Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties | Lines of communication for quantum cyber risk should address stakeholders at multiple layers of cryptographic impact across the organization (e.g., management of cryptographic algorithms and modules, cryptographic protocols and assets, through to data, systems, applications and up to protected communication channels and impacted business processes).<br><br>Establishing a cryptographic center of excellence (CCoE), or other centralized organizational body, can facilitate coordination and communication regarding quantum cyber risk.<br><br>Designating a senior official for cryptographic migration and risk management can minimize confusion and conflicting initiatives regarding QRC initiatives. |
| GV.RM-06 | A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated | Methods for calculating, documenting, categorizing, and prioritizing cybersecurity risk should account for quantum cyber risk, as well as risk and costs associated with cryptographic debt and rigidity.<br><br>Methods for calculating, documenting, categorizing, and prioritizing quantum cyber risk should, at minimum, account for whether cryptography is vulnerable to a CRQC (e.g., asymmetric cryptography), whether data is at-risk from CRQC-based attacks (data with a shelf life that makes it a target for Harvest Now Decrypt Later (HNDL) attacks, or would be prioritized for compromise by an advanced adversary with an early CRQC), and system criticality (e.g., high value asset).<br><br>Methods for calculating, documenting, categorizing, and prioritizing risk associated with cryptographic debt should, at minimum, account for the risk |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| | | and costs of maintaining legacy cryptographic systems, and of mitigating risk associated with a lack of adequate, or no, cryptographic protections.<br><br>In order to adequately inform QRC migration, risk prioritization should account for: (a) status of applicable cryptographic governance (e.g., policies and procedures for cryptographic management, level of cryptographic monitoring); (b) impacted mission and business processes, data, applications/systems, protocols, and algorithms; (c) mitigating factors (e.g., multiple layers of protection, internal-only access); (d) system lifecycle context (e.g., system scheduled for modernization); and (e) characteristics of vulnerable cryptography and cryptographic assets (e.g., custom or off-the-shelf, including details of any vendor's QRC maturity). Organizations should consider cost and feasibility of QRC migration when evaluating these factors for a given system. For example, prioritizing QRC implementations for new systems and for assets that currently do not implement cryptographic protections may allow for faster implementation and lower interoperability risk when compared to migrating systems with high cryptographic debt. |
| GV.RM-07 | Strategic opportunities (e.g., positive risks) are characterized and are included in organizational cybersecurity risk discussions | Quantum cyber risk discussions and prioritization should account for opportunities to modernize systems to enable greater cryptographic agility (including cloud migration, and re-platforming). |
| GV.RR-01 | Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving | Organizations should designate a senior official for cryptographic migration and risk management; and should establish cross-functional organizational bodies that foster collaboration on quantum cyber readiness across enterprise leadership (including Privacy and Secure Supply Chain leadership).<br><br>Clear sponsorship and accountability for the topic of cryptography, and specifically quantum cyber risk, should be established.<br><br>Collaboration can be fostered across leadership through a CCoE, and through incorporation and elevation of quantum cyber risk on other organizational committees and oversight bodies (including, where applicable, within the board). |
| GV.RR-02 | Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced | Roles, responsibilities, and authorities related to cryptography risk management and QRC migration should be incorporated into roles, responsibilities, and authorities of existing cybersecurity and information technology personnel where feasible. This can include reflecting cryptography management in the org chart, and recognizing a governance structure which is fit-for-purpose and adheres to identified risks (as opposed to a one size fits all approach). |
| GV.RR-03 | Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies | Resource planning for QRC migration should be informed by quantum cyber readiness assessment, based on broad cryptographic discovery.<br><br>Costs of QRC migration should be accounted for as part of multi-year budget planning and incorporated into complementary initiatives such as system modernization (e.g., cloud migration) and Zero Trust. Costs savings from proactively addressing cryptographic agility in system development and modernization should be incorporated into budget decisions and prioritization.<br><br>Costs and budget estimates for QRC migration should include total replacement or modernization costs associated with assets for which implementation of QRC is not possible or feasible. |
| GV.RR-04 | Cybersecurity is included in human resources practices | QRC- and legacy cryptography-related roles should be considered sensitive and afforded appropriate security classification and vetting. |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| GV.PO-01 | Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced | Quantum cyber risk, QRC, and cryptographic agility should be incorporated into organizational policies for managing cybersecurity risk.<br><br>Policy compliance should be tested and enforced on an ongoing basis through independent assessments, internal testing (including automated cryptographic and vulnerability scanning), and training. |
| GV.PO-02 | Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission | QRC-related policy should be updated on an ongoing basis, based on results of assessment and testing, and in response to emerging standards and guidance.<br><br>Enterprise policies should prioritize cryptographic agility throughout the IT lifecycle so that requirements can be more easily and consistently updated and communicated in response to changes. This action should establish both new, dedicated policies, as well as add consideration from cryptographic risk to existing policies (e.g., Software Development Lifecycle, procurement). |
| GV.OV (Category-level only) | Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy | The Quantum Cyber Readiness roadmap is reviewed and adjusted based on results of ongoing cryptographic discovery and inventory, external and internal assessments, as well as piloting of, and progress towards, QRC migration and implementation of cryptographically agile architectures. |
| GV.SC-01 | A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders | Cybersecurity supply chain risk management program, strategy, objectives, policies, and processes should address cryptographic resilience and QRC. |
| GV.SC-02 | Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally | A shared responsibility model for cryptographic resilience and QRC migration should be established to delineate roles and responsibilities for suppliers, customers, and partners. Due to the interconnected nature of cryptography, and the high concern for interoperability risk associated with implementation of QRC and transition to cryptographic agility, it may be necessary for roles and responsibilities to be shared and delineated across CSF Subcategories, in addition to within specific activities.<br><br>For QRC products where independent verification and validation of conformance to QRC standards and performance testing is not available, organizations should coordinate with suppliers and other third parties to conduct testing and validation prior to implementation in production environments. |
| GV.SC-03 | Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes | Cryptographic supply chain risk management should inform cybersecurity and enterprise risk management, as well as IT modernization and acquisition strategy and processes. |
| GV.SC-04 | Suppliers are known and prioritized by criticality | Organizations should include details identifying suppliers of CRQC-vulnerable assets in their cryptographic inventories. They should also prioritize identifying responsible parties for remediating quantum cyber risks and migrating to QRC.<br><br>Suppliers of hardware security modules (HSM), public key infrastructure (PKI), or of hardware and equipment with embedded cryptography (e.g., in |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| | | firmware), should be prioritized for monitoring and QRC migration planning.<br><br>Where information about cryptographic resilience is not readily available from suppliers (e.g., through centralized reporting or third parties), organizations should engage suppliers to determine which products with CRQC-vulnerable cryptography will not support or be able to migrate to QRC, and determine options for transitioning to alternate solutions. |
| GV.SC-05 | Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties | Cryptographic Bills of Materials (CBOM), as well as cryptographic discovery and inventory, should be integrated into supplier and third-party requirements.<br><br>Organizations should consider requiring third parties to provide quantum cyber readiness plans and attestations that demonstrate scope and schedule for QRC migration, as well as conformance to QRC standards. |
| GV.SC-06 | Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships | For critical products and services containing CRQC-vulnerable cryptography, conformance to QRC standards, or plans for QRC migration, should be verified prior to acquisition.<br><br>Where feasible, organizations should leverage independent third-party evaluation for due diligence.<br><br>Organizations should consider insurance and liability associated with cryptographic vulnerabilities as part of agreements with suppliers and third parties. |
| GV.SC-07 | The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship | Organizations should conduct periodic evaluations of critical suppliers, their products and services, and other third parties, for cryptographic risk and resilience (including progress towards QRC implementation).<br><br>Organizations should require third parties to report cryptographic compromise or risks in a timely matter, and provide mitigation and remediation plans as appropriate.<br><br>For third-party solutions, CBOM and cryptographic discovery and inventory should be maintained continuously and updated whenever significant changes occur. |
| GV.SC-08 | Relevant suppliers and other third parties are included in incident planning, response, and recovery activities | Organizations should include suppliers and third parties responsible for cryptographic assets and services in incident management activities for quantum cyber readiness. Table-top and continuity of operations (COOP) exercises that address cryptographic compromise associated with a CRQC or migration to QRC can be essential tools for quantum cyber readiness. |
| GV.SC-09 | Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle | Mitigation of quantum cyber risk associated with suppliers and third parties should be integrated into cybersecurity and enterprise risk management programs, including disaster recovery and crisis management. |
| GV.SC-10 | Cybersecurity supply chain risk management (SCRM) plans include provisions for activities that occur after the conclusion of a service agreement | Organizations should include provisions in their SCRM plans for identifying when cryptographic assets are no longer supported by a supplier. Additionally, they should outline how monitoring and mitigation will be performed by the organization thereafter.<br><br>Where feasible, organizations should require that a supplier's obligations to timely report cryptographic compromise survive any contract or agreement. |

 

Identify

The Identify (ID) Function emphasizes the critical importance of understanding an organization's current cybersecurity risks. It includes the following Categories, which provide key performance outcomes as part of a broad cyber risk management framework:

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
- **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization.
- **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.

As detailed in the table below, each of the Identify Categories and associated Subcategories are critical for effective cryptographic resilience as organizations advance their quantum cyber readiness. Specifically, they provide the critical foundation for recognizing and cataloging the assets, systems, data, and capabilities that need protection. This includes identifying quantum-related vulnerabilities and threats, assessing the potential impact on cryptographic systems, and understanding the organizational environment. Due to the high effort and long timelines associated with QRC migration and transition to cryptographic agility, proactive identification and planning related to these assets is critical for quantum cyber readiness.

*Table 3: CSF 2.0 Community Profile – Identify*

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| ID.AM-01 | Inventories of hardware managed by the organization are maintained | Organizations should maintain inventories of hardware that provide cryptographic services (e.g., HSM), or that rely on CRQC-vulnerable cryptography; and for such hardware, identify cryptographic components and associated suppliers.<br><br>Inventories should be developed and maintained using automated discovery capabilities and updated on an ongoing basis. Organizations should broadly consider existing capabilities that can be repurposed or enhanced for cryptographic discovery, as well as new dedicated tools. |
| ID.AM-02 | Inventories of software, services, and systems managed by the organization are maintained | Organizations should maintain inventories of software that provide cryptographic services (e.g., PKI), or that rely on CRQC-vulnerable cryptography; and for such software, identify cryptographic components, and associated suppliers.<br><br>Inventories should be developed and maintained using automated discovery capabilities and updated on an ongoing basis. Organizations should holistically consider existing capabilities that can be repurposed or enhanced for cryptographic discovery, as well as new dedicated tools. |
| ID.AM-03 | Representations of the organization's authorized network communication and internal and external network data flows are maintained | Cryptographic discovery should identify cryptography and data in transit and in use throughout the enterprise and should include cryptographic interoperability considerations associated with system interconnections. |
| ID.AM-04 | Inventories of services provided by suppliers are maintained | Organizations should include in their cryptographic inventories details identifying suppliers of CRQC-vulnerable assets, and prioritize identification of responsible parties for remediation of quantum cyber risks and migration to QRC.<br><br>Organizations should obtain and maintain CBOMs for products and services depending on CRQC-vulnerable cryptography. |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| ID.AM-05 | Assets are prioritized based on classification, criticality, resources, and impact on the mission | Assets should be prioritized for QRC migration based on: (a) risk indicators associated with the data and systems they impact (e.g., whether data is at-risk from HNDL attacks due to having a long shelf life, or whether data or systems have a high adversarial value and would therefore be prioritized for compromise by an advanced adversary with an early CRQC), (b) impacted mission and business processes, including cost, (c) mitigating factors (e.g., multiple layers of protection, internal-only access), (d) system lifecycle context (e.g., system scheduled for modernization), as well as (e) characteristics of CRQC-vulnerable cryptography and cryptographic assets (e.g., custom or off-the-shelf, including details of any vendor's QRC maturity). |
| ID.AM-07 | Inventories of data and corresponding metadata for designated data types are maintained | Organizations should maintain inventories of data that are protected by CRQC-vulnerable cryptography and, for such data, identify data types, sensitivity, and shelf-life for the data to remain sensitive.<br><br>Inventories should be developed and maintained using automated discovery capabilities and updated on an ongoing basis. Organizations should holistically consider existing capabilities that can be repurposed or enhanced for cryptographic discovery, as well as new dedicated tools. |
| ID.AM-08 | Systems, hardware, software, services, and data are managed throughout their life cycles | Cryptography should be managed throughout system, hardware, software, services, and data lifecycles.<br><br>Cryptography management should prioritize migration of assets to QRC and transition to cryptographic agility, and should be informed by automated cryptographic discovery and risk assessment. |
| ID.RA-01 | Vulnerabilities in assets are identified, validated, and recorded | Cryptographic vulnerabilities and risks should be identified, validated, and recorded on an ongoing basis, including through implementation of a broad cryptographic discovery methodology that leverages automated cryptographic discovery and analysis tools. |
| ID.RA-02 | Cyber threat intelligence is received from information sharing forums and sources | Organizations should establish mechanisms for receiving and integrating cyber threat intelligence related to quantum computing threats into cyber incident response. There will likely be limited indicators of cryptographic compromise by a CRQC, and insights into adversaries' capabilities and targets should they obtain a CRQC are not widely known; therefore, reliance on advanced threat intelligence sources will be critical to inform defensive action. |
| ID.RA-03 | Internal and external threats to the organization are identified and recorded | Non-malicious threats to systems and data resulting from improper cryptographic management, poor QRC migration planning, and interoperability challenges should be identified and monitored for both internal and external systems. |
| ID.RA-04 | Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded | Impact and likelihood of threats to availability and integrity of systems and data due to cryptographic compromise should be identified and recorded, in addition to threats to confidentiality. In many cases, availability and integrity threats should be prioritized due to the wide-scale scope of harm.<br><br>The impact of cryptographic compromise on system availability due to a CRQC attack may be immediately catastrophic and result in the complete failure of systems and digital communications, which may include serious tangible harm. The impact of cryptographic compromise on system integrity may result in a complete loss of digital trust that undermines the functionality of digital transactions and confidence in critical institutions. |
| ID.RA-05 | Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization | Threats, vulnerabilities, likelihood, and impacts should inform both implementation of QRC and deprecation of legacy cryptographic algorithms, including prioritization and timelines.<br><br>Threat and impact information alone, however, is unlikely to provide adequate context to plan an actionable roadmap for quantum cyber readiness. Given the depth and breadth of CRQC-vulnerable cryptography across an enterprise, planning and prioritization for QRC migration should be |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| | | tailored to an organization's mission and business needs, and differentiated across assets to account for feasibility and cost of QRC migration and transition to cryptographic agility. |
| ID.RA-06 | Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated | Organizations should consider hybrid implementations of QRC, which allow for maintaining legacy cryptography during the transition to QRC. In such cases, dual risk acceptance and mitigation decisions may be warranted. |
| ID.RA-07 | Changes and exceptions are managed, assessed for risk impact, recorded, and tracked | Organizations should include cryptographic impact assessments within change control processes and procedures, and should monitor QRC implementations to verify that changes do not roll back assets to CRQC-vulnerable cryptography. |
| ID.RA-08 | Processes for receiving, analyzing, and responding to vulnerability disclosures are established | Processes for receiving, analyzing, and responding to discovery of CRQC-vulnerable cryptography should be established. |
| ID.RA-09 | The authenticity and integrity of hardware and software are assessed prior to acquisition and use | Traditional methods for assessing authenticity and integrity may not be trustable considering the threat posed by a CRQC; QRC-enabled certificates and robust cryptographic supply chain risk management are essential for maintaining trust in asset authenticity and integrity. |
| ID.RA-10 | Critical suppliers are assessed prior to acquisition | Critical suppliers' conformance to QRC standards and maturity of cryptographic agility should be assessed prior to acquisition. |
| ID.IM (Category-level only) | Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions | Improvements to cryptographic risk management and quantum cyber readiness processes and procedures should be identified across all CSF Functions, should incorporate feedback from continuous evaluation and assessment (including self-assessments), and should be reflected in QRC implementation plans. |

 

## Protect

The Protect (PR) Function emphasizes the critical importance of using safeguards to manage the organization's cybersecurity risks. It includes the following Categories, which provide key performance outcomes as part of a broad cyber risk management framework:

- **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.
- **Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.
- **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.
- **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability as well as organizational resilience.

As detailed in the table below, each of the Protect Categories are critical for effective cryptographic resilience as organizations advance their quantum cyber readiness. Specifically, they encompass the essential actions and controls necessary to promote the integrity, confidentiality, and availability of information systems and data in the face of threats to cryptography. This includes, first and foremost, a prioritized implementation of QRC and cryptographic agility within and across digital systems.

Importantly, while the overarching Protect Categories are covered below, this Profile does not address each of the Subcategories in detail. It focuses on the broader strategic actions that organizations should prioritize to achieve quantum cyber readiness, rather than the specific technical implementations that can vary significantly based on individual organizational needs and contexts. This is all the more important given the evolving standards and implementation requirements for QRC, including ongoing performance and interoperability testing. By prioritizing these higher-level protective measures, organizations can maintain focus on foundational performance outcomes to fortify their defenses, mitigate risks, and maintain resilience in the face of evolving quantum cyber threats, setting themselves up for success in later phases of implementation that may involve more granular technical requirements.

*Table 4: CSF 2.0 Community Profile – Protect*

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| PR.AA (Category-level only) | Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access | Cryptographic authenticators and credentials should utilize QRC, commensurate with risk of unauthorized access. |
| PR.AT (Category-level only) | The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks | Cryptographic risk and impacts should be incorporated into general and role-based security awareness training, related to supply chain, acquisition and third-party risk management, in particular. As part of proactive quantum cyber risk management, such training should be prioritized for certain roles responsible for planning and monitoring associated with the migration to Quantum Resistant Cryptography (e.g., acquisitions personnel). |

 

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| PR.DS (Category-level only) | Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information | Data in transit, at rest, and in use, should be protected using QRC throughout the data lifecycle (e.g., across and within systems, and communications channels, and in memory). QRC and quantum resistant cryptography should be implemented at the data, database, and application layers to provide adequate defense in depth; implementation of QRC at the hardware and network layers alone (including relying solely on QRC-enabled VPNs) may not be sufficient to protect data from quantum threats.<br><br>Data that is CRQC-vulnerable to quantum threats, and which will remain mission sensitive for extended timeframes, should be prioritized for QRC migration. This should include data previously destroyed via cryptographic erasure using CRQC-vulnerable cryptography. |
| PR.PS-01 | Configuration management practices are established and applied | Cryptographic management practices that facilitate cryptographic agility and resilience should be established and applied. |
| PR.PS-02 | Software is maintained, replaced, and removed commensurate with risk | Cryptography in software is migrated to QRC commensurate with risk; and where not feasible, software is replaced and removed, or applications are re-platformed and redeveloped to support QRC and facilitate cryptographic agility. |
| PR.PS-03 | Hardware is maintained, replaced, and removed commensurate with risk | Cryptography in firmware is migrated to QRC commensurate with risk and, where not feasible, hardware is replaced and removed. |
| PR.PS-04 | Log records are generated and made available for continuous monitoring | Access and changes to cryptographic assets should be logged and prioritized for monitoring. Changes to cryptographic assets should be accounted for in cryptographic discovery, and should inform updates to cryptographic inventories and QRC migration planning. |
| PR.PS-05 | Installation and execution of unauthorized software are prevented | Implementation of unauthorized cryptography should be prevented and monitored. |
| PR.PS-06 | Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle | System architectures and development practices that promote cryptographic agility should be prioritized and enforced throughout the system development lifecycle. |
| PR.IR (Category-level only) | Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience | QRC and cryptographic agility should be implemented for networks, commensurate with risk, to protect asset confidentiality, integrity, and availability. Performance and interoperability testing for QRC should be conducted as part of system development, and should account for system resource impacts, interconnections, and third-party compatibility; and risks should be addressed prior to implementing infrastructure changes.<br><br>Cryptography protection measures should be included and maintained in security architectures. |

 

## Detect, Respond & Recover

The Detect (DE), Respond (RS), and Recover (RC) Functions emphasize the critical importance of finding and analyzing possible cybersecurity attacks and compromises, taking action regarding a detected cybersecurity incident, and restoring assets and operations affected by a cybersecurity incident. They include the following Categories: Continuous Monitoring (DE.CM), Adverse Event Analysis (DE.AE); Incident Analysis (RS.AN), Incident Response Reporting and Communication (RS.CO), Incident Mitigation (RS.MI); Incident Recovery Plan Execution (RC.RP), Incident Recovery Communication (RC.CO).

While the ability to detect, respond to, and recover from quantum-related cyber threats is critical for effective cryptographic resilience as organizations advance their readiness, it is not high priority for many organizations today due to the evolving nature of threats and uncertainty surrounding the timeline for emergence of a CRQC. The priority lies in fortifying defenses and preventing incidents from occurring in the first place, including through proactive measures, such as conducting cryptographic discovery and implementing QRC.

That said, this Profile incorporates the Continuous Monitoring (DE.CM) Category within the Detect Function as a priority due to its impact on other quantum cyber readiness activities. Performance outcomes under this Category can meaningfully contribute to effective cryptographic resilience when organizations incorporate cryptography and quantum cyber risks into their broader cyber threat monitoring.

Importantly, in many organizations, the tools used to conduct monitoring for threat detection and vulnerability management under this Function are the same that can - and should - be used for automated cryptographic discovery and risk analytics. Integrating and correlating risk management activities across this Function can provide critical efficiencies, risk insights, and potential cost savings.

*Table 5: CSF 2.0 Community Profile – Detect*

| CSF 2.0 Core Categories | CSF 2.0 Performance Outcomes | Recommendations and Considerations for Cryptographic Resilience |
|---|---|---|
| DE.CM (Category-level only) | Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events | Monitoring of cryptographic risk should be performed across all system layers, and should account for data, file systems, applications, networks, and hardware for both internal and external (third-party) systems.<br><br>Monitoring should include periodic assessment as well as ongoing automated cryptographic discovery. |

 

# References

**Sources and Mappings.** Subsequent versions of this profile will contain informative reference and mappings to specific sources and authorities for each core outcome. This mapping will provide crosswalk relationships that can help users achieve the CSF 2.0 performance outcomes or that can inform assessments of performance outcomes that their organization is already achieving (e.g., industry standards or guidelines).

**Endnotes.** Specific references and notes cited in this document are listed below:

---

[1] NIST Cybersecurity White Paper (CSWP) 29, The NIST Cybersecurity Framework (CSF) 2.0 (February 26, 2024).

[2] Migration to QRC involves implementation of NIST-standardized cryptographic algorithms recommended as being sufficiently secure against adversaries in possession of the CRQC, currently FIPS 203, 204, 205. Cryptographic agility refers to capabilities that enable an organization to quickly replace and adapt cryptographic algorithms in protocols, applications, software, hardware, and infrastructures without compromising the operation of a system.

[3] NIST IR 8547 ipd (Initial Public Draft), Transition to Post-Quantum Cryptography Standards (November 2024); NIST CSWP 39 ipd (Initial Public Draft), Considerations for Achieving Crypto Agility (March 5, 2025).

[4] Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, Version2.0 (April 2023); see also, Deloitte Quantum Trust Maturity Model, available at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-quantum-trust-maturity-model-july-2023.pdf

To learn more, visit www.deloitte.com/quantumcyber, or contact our team today.

**Colin Soutar**
Global Quantum Cyber Readiness Leader
Managing Director
Deloitte & Touche LLP
csoutar@deloitte.com

**Benjamin Shapiro**
Senior Manager
Deloitte & Touche LLP
beshapiro@deloitte.com

 